REMARKS

This responds to the Office Action mailed on September 15, 2003. Applicant has made no changes to the claims.

§102 Rejection of the Claims

Claims 1-35 were rejected under 35 USC § 102(a) as being anticipated by Thomsen et al. (Role Based Access Control Framework for Network Enterprises) (hereinafter "Thomsen").

Thomsen describes a Role Based Access Control (RBAC) mechanism for managing access to a variety of network resources. As the Examiner notes, Thomsen describes a system in which application-specific security mechanisms are encapsulated into keys (Section 4.2) and the keys are linked to form key chains (Section 2.6). Thomsen states that key chains may contain other key chains.

As can be seen in Fig. 4 of the drawings, Applicant teaches that an RBAC model can be constructed that includes an application developer layer (30), one or more semantic layers (36) and a local system administrator layer 32. The goal of the application developer layer is to encapsulate application specific information so that it can be incorporated into the higher layers in a uniform manner. Once the application specific information has been encapsulated into an application key, it can be combined with other keys to form semantic layers 36 such as are shown in Fig. 7. Each layer 36 starts with a set of keys 40 and uses them to build up key chains 42 representing the policy at that level. Once key chains have been built, constraints 44 may be associated with them. The key chains for one layer become keys 40 of other layers 36. Within a layer 36 keys 40 are atomic units of policy. By drilling down to another layer 36 the user can determine how the key was composed.

The final layer of RBAC model described by Applicant is identical to the other layers except that at this level users can be associated with key chains. The top layer is the only layer where such user role binding takes place. The top layer is also assumed to be under the control of the local sysadmin. As noted above, the top layer is more dynamic than the lower layers as it must respond to the day-to-day operations of the network.

Thomsen does not consider, or even mention, the use of semantic layers to combine keys into key chains, as described by Applicant and claimed in claims 1-35. Nor does Thomsen

describe why or how one would encapsulate key chains as keys within a semantic layer or why or how one would pass the encapsulated chains to the next semantic layer. These features of an RBAC system are described by Applicant and claimed in claims 1-5, 14-35.

Furthermore, Thomsen does not describe the use of a plurality of semantic layers or a user interface for defining a security policy as a function of keys received from lower semantic layers as described by Applicant and claimed in claims 6-10.

Furthermore, Thomsen does not describe a tool for manipulating the RBAC model as described by Applicant and claimed in claims 11-13.

Reconsideration of all claims is respectfully requested.

Claims 1-3, 5-8, 14-16, 22-24, 30, and 32-34 were rejected under 35 USC § 102(b) as being anticipated by Crall et al. (Issues in the Design of Secure Authorization Service for Distributed Applications, 1998) (hereinafter "Crall").

Crall describes a RBAC system. Crall describes a system in which entitlements define access rights for principals. Profiles are used to provide the same privileges to groups or classes of principals. In the example given at page 879, an administrator creates a profile called Teller that defines all the privileges granted to bank tellers. A principal that becomes a member of the Teller profile automatically has all the privileges assigned in it. The Examiner stated that privileges "represent authorization to access application-specific resources" and that "entitlements" are "encapsulated privileges" that "represent authority to perform tasks".

Applicant disagrees. Crall's entitlements are not encapsulated privileges. Applicant teaches that each key represents the ability to access some resource. One can use an entitlement as defined by Crall to define an ability to access some resource, but there is no encapsulation as defined by Applicant and claimed in claims 1-35. Instead, Crall defines a principal's privileges in terms of privileges defined for the individual, privileges assigned to any profiles associated with the individual and privileges assigned to the entitlement. Therefore, one must review each of these areas when modifying access rights of the individual.

The Examiner further states that "entitlements can be combined through Boolean expressions". Applicant is unable to find any evidence of this in the reference. Instead, Crall indicates that "rule elements within the entitlement can be combined in an entitlement rule using AND and OR logical expressions and nested parenthesized expressions." P. 879, lines 1-8.

Therefore, Crall cannot teach the key chaining concept described by Applicant and claimed in claims 1-5 and 13-35.

Furthermore, Crall does not consider, or even mention, the use of semantic layers to combine keys into key chains, as described by Applicant and claimed in claims 1-35. Nor does Crall describe why or how one would encapsulate key chains as keys within a semantic layer or why or how one would pass the encapsulated chains to the next semantic layer. These features of an RBAC system are described by Applicant and claimed in claims 1-5, 14-35.

Furthermore, Crall does not describe the use of a plurality of semantic layers or a user interface for defining a security policy as a function of keys received from lower semantic layers as described by Applicant and claimed in claims 6-10.

Furthermore, Crall does not describe a tool for manipulating the RBAC model as described by Applicant and claimed in claims 11-13.

Reconsideration of all claims is respectfully requested.

Claims 36-38 were rejected under 35 USC § 102(b) as being anticipated by Barkley (U.S. Patent No. 6,088,679).

Barkley describes a method of using roles to perform activities in a workflow system. Under Barkley, a workflow is decomposed into sequential and parallel segments. Roles are created corresponding to each activity within each segment and permission to perform the operations of that activity are assigned to the corresponding roles. An individual is assigned to each role; the roles are then activated so the individual can perform the activity. The roles are then deactivated as each segment is completed.

Applicant teaches, and claims in claims 36-38, that workflow can be controlled by creating a workflow class definition and exporting the workflow class definition to a central policy management system. Barkley does not export a workflow class definition to a central policy management system. Instead, as best as Applicant can determine, Barkley decomposes the workflow definition into segments within the workflow management system (col. 6, line 42 through col. 7, line 51), defines roles each activity within each segment and provides a mechanism for enforcing the privileges assigned to each role outside the workflow management system. This is a different approach from that taken by Applicant and claimed in claims 36-38.

Reconsideration of claims 36-38 is respectfully requested.

§103 Rejection of the Claims

Claims 4, 9, 10, 11-13, 17, 25-26 and 31 were rejected under 35 USC § 103(a) as being unpatentable over Crall et al. in view of Sandhu et al. (The ARBAC97 Model for Role-Based Administration of Roles).

Crall is discussed above.

Sandhu describes a role-based model for RBAC administration.

The Examiner notes that Crall "lacks a means for drilling to a lower layer to customize security policies." In fact, as noted above, Crall does not even contemplate an RBAC system having a plurality of semantic layers. The Examiner states that Sandhu discloses a structure ("UP-role") that includes abilities and permissions. Sandhu defines abilities as "roles that only have permissions and other abilities as members." Neither reference discloses the use of multiple semantic layers as described by Applicant and claimed in claims 4, 9 and 10.

The Examiner stated that Sandhu discloses the use of constraints in an RBAC system. Applicant speaks to this as well in the Background section of the application. Neither reference discloses, however, the application of constraints within semantic layers as described by Applicant and claimed in claims 11, 17, 25 and 26.

Claims 12 and 13 are dependent on claim 11 and inherit all the limitations of claim 11. They are allowable for the reasons provided in discussing claim 11 above.

Claims 18 and 19 are dependent on claim 14 and inherit all the limitations of claim 14. They are allowable for the reasons provided in discussing claim 14 above.

Claims 27 and 28 are dependent on are dependent on claim 22 and inherit all the limitations of claim 22. They are allowable for the reasons provided in discussing claim 22 above.

Claims 31 and 35 were rejected under 35 USC § 103(a) as being unpatentable over Crall et al. in view of Sandhu et al. in further view of Samarati (Access Control: Principles and Practice, 1994).

As noted above, none of the references cited by the Examiner contemplate an RBAC system having a plurality of semantic layers. The Examiner states that Sandhu discloses

organizing roles in a partial order (in order to foster inheritance) but that neither reference discloses displaying the partial ordering as a role hierarchy graph. The Examiner states that Samarati does provide such a disclosure.

As noted by Applicant at p. 17, lines 20-28:

> The drawbacks of eliminating role inheritance can be mitigated by a hybrid approach that constructs a role hierarchy from the lists of keys. In such an embodiment, each key chain 42 is a set of keys 40; GUI 22 sorts the key chains into a partial ordering based on set containment. For example, a key chain with keys {a, b, c} is more powerful than a key chain with {b, c}. Key chains with the most keys appear on top, key chains with fewer keys on the bottom. Once the partial ordering is calculated the information is shown to the sysadmin via a standard role hierarchy graph. The benefit of this approach is that the sysadmin does not have to maintain the role to role relationships explicitly, the tool constructs the role hierarchy for the user.

Applicant has reviewed the section cited by the Examiner and is unable to see a teaching that would lead one to construct a role hierarchy by sorting the key chains into a partial ordering based on set containment, display the partial ordering as a role hierarchy graph and add and delete keys from the role hierarchy graph, as described by Applicant and claimed in claims 31-35. Reconsideration of claims 31-35 is respectfully requested.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney at (612) 373-6909 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

DANIEL J. THOMSEN ET AL.

By their Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
Attorneys for Intel Corporation
P.O. Box 2938
Minneapolis, Minnesota 55402
(612) 373-6909

Date March 15, 2004

By Thomas J. Brennan
Thomas F. Brennan
Reg. No. 35,075

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 15th day of March, 2004.

Thomas F. Brennan
Name

Thomas J. Brennan
Signature